# The Future of Cardless Broadcast Security

## A Farncombe White Paper on Key Trends in the Approach to Video Security

Sponsored by Verimatrix

October 2012

farncombe

Liberty House | 222 Regent Street | London, W1B 5TR
T +44 (0)207 297 2002 | F +44 (0)207 207 2100 | www.farncombe.com

# Table of Contents



# 1. Introduction: CA Systems vs. Piracy

## 1.1 Aims of this paper

In our previous paper, *TV Conditional Access Systems in Two-Way Environments*[1], we discussed the implications of an "always-on" return path for CA systems. In this paper, we look at how changes in piracy and technology are affecting the implementation of CA systems in the more common *one-way* broadcast network and – more specifically – how the relevance of cardless security to one-way service operators is changing.

To answer these questions, Farncombe has looked at the following issues:

- How are new card-based and cardless technologies changing the level of protection offered against piracy, and how is the threat of piracy changing?
- How are market changes affecting the nature of the threats?
- What factors affect the total cost of ownership of a CA system?
- Under what circumstances is a cardless system appropriate for use in a one-way network?

## 1.2 How cardless and card-based CA systems prevent piracy

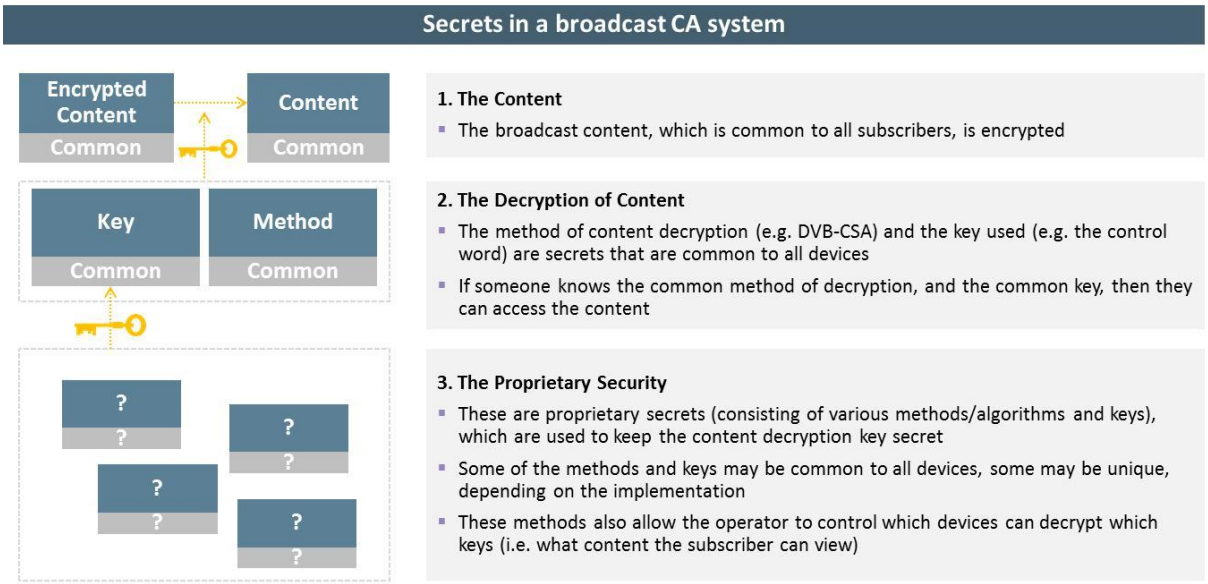
### Secrets in a broadcast network

One-way broadcast security systems, as with any security systems, rely upon the ability to protect secrets, but with the added difficulty that the secrets are common to, and must be shared with, thousands – if not millions – of devices.

> *"Two can keep a secret,*
>
> *if one of them is dead"*
>
> **Benjamin Franklin**

Figure 1 shows the secrets involved in a broadcast CA system, consisting of the content itself, the content's decryption, and the proprietary security techniques employed by the CA vendor. Figure 1 shows how the decryption of content uses a common key and a common method – an inherent weakness in one-way broadcast systems.

**Figure 1: Secrets in a broadcast network**




*Source: Farncombe*

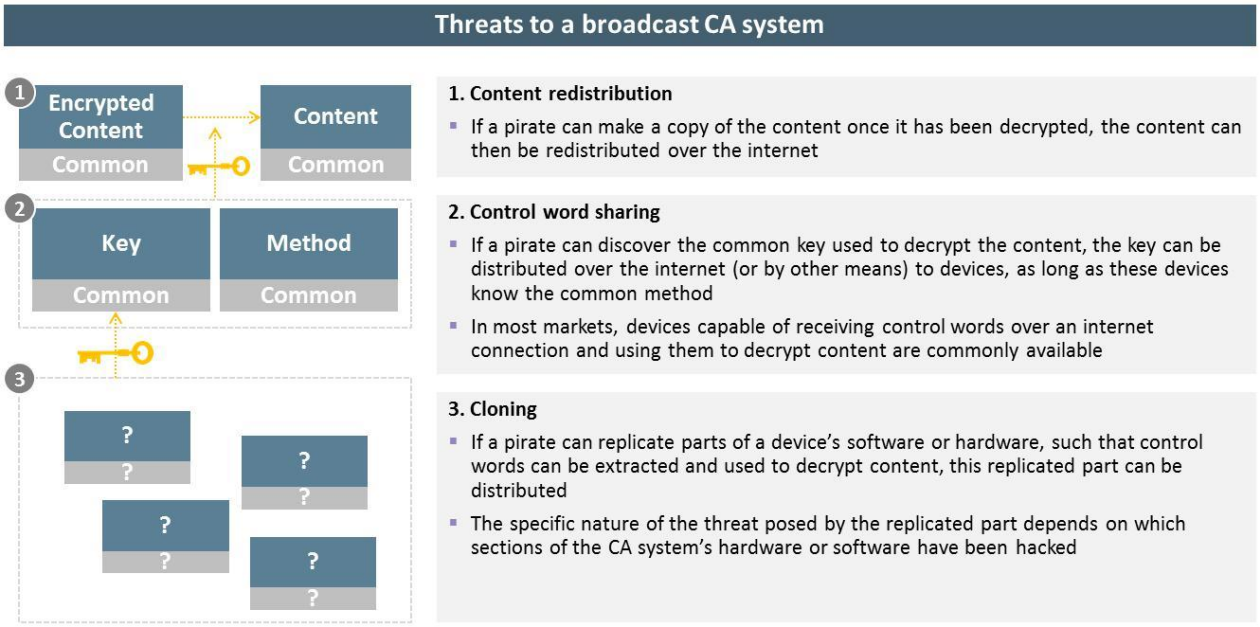
[1] http://bit.ly/V0o7yI

## Threats: the discovery of secrets

The threat of a security hack to the operator depends on **which secrets are discovered by the pirate.** These threats fall into three categories (as shown in Figure 2): Content redistribution; Control-word sharing; and Cloning.

Each type of threat poses a different set of challenges to the pirate and has different implications for the operator.

**Figure 2: Threats to CA systems**




*Source: Farncombe*

## Summary of Cardless[2] vs. Card-based protection against piracy

The details of these challenges and implications, and how they differ between cardless and card-based CA systems are discussed in the Appendix. For the purposes of this White Paper, five conclusions should be well understood:

1. When attacking a CA system, pirates have to weigh up the **barriers** to an attack (in terms of time and cost) and the potential **rewards** of the attack (in terms of operator reach and value of content).
2. Neither cardless nor smartcard-based systems will ever improve sufficiently to prevent all attacks – given enough time and money, a successful attack is always possible. However, **improvements in the technologies** used in cardless CA systems will (when implemented correctly) create barriers sufficient that most attacks will only affect operators whose content is of high value to pirates and which is not accessible elsewhere.
3. Regardless of CA system, in a territory with good broadband connectivity **content redistribution** represents an easy way for a pirate to steal content, and can only be responded to through monitoring and shutting down the pirate services. This reduces the value of attacking the CA system, increasing the potential scope of use of cardless CA systems.
4. Both card-based and cardless CA systems will suffer from **control-word sharing** attacks, though smartcard solutions that make use of an unprotected interface would be more susceptible to these attacks. Regardless of CA system type, the attack can be responded to through the monitoring and closing down of pirate services which, when combined with enforcement action, has been sufficient to avoid device replacement.

[2] In this paper, where we discuss cardless CA systems, we are referring to those with a combined software and hardware implementation, as described in the Appendix

5. Cardless CA systems will also suffer from the additional threat of **perfect cloning**. Suitable responses to this are: 1) to replace all devices; or 2) to migrate to a smartcard system *if an unused smartcard slot is present*. Perfect cloning requires significant resource (including time) on the part of the hacker, but if the incentive for such a hack exists, we can assume that it will eventually take place. Note that some 1-way cardless CA systems implement tools to detect and stop cloning attacks even without a return path. Clones that reveal their identity can be detected and disabled; however, if new clones can be developed rapidly or their identity is hard to find, then the threat cannot be removed.

# 2. The Changing Threat Model

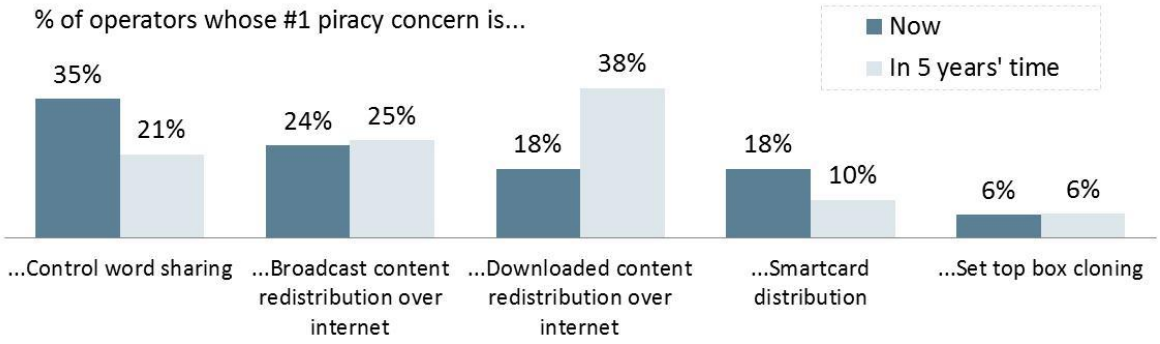
## 2.1 Changing weak points

### The rise of content redistribution as a threat

Prior to the mass-adoption of broadband, cloning was the most common of the three piracy threat-types discussed in this paper. However, as broadband penetration has grown, the distribution of control-words over an internet connection has become less of a barrier to pirates: according to Farncombe's Security and Piracy Survey[3], conducted in August 2012, the primary concern of pay-TV operators is now control-word sharing.

This situation is set to change again as broadband availability increases. According to the Security and Piracy Survey, pay-TV operators believe that content redistribution will become the main piracy threat over the next five years.

**Figure 3: Operator piracy concerns**

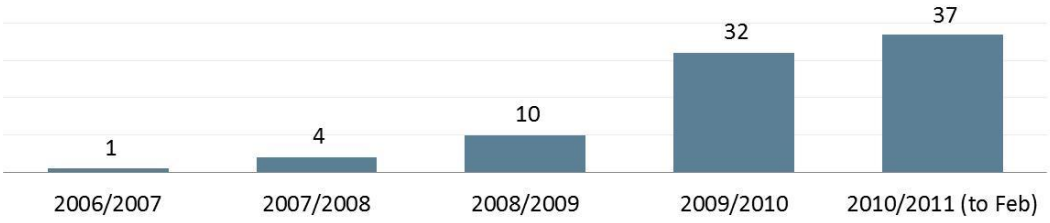



*Source: Farncombe Security and Piracy Survey*

The view of operators is supported by data from across the industry. The growth in the streaming of premium content has been dramatic, as broadband speeds have increased and as sites offering cheap (and sometimes even free) streaming have multiplied.

Figure 4 illustrates the widespread availability of streamed pirated content. The number of sites shown represents only UGC sites, where pirates can set up a stream at no cost – content is also distributed through P2P software, CDNs and direct one-to-one streaming. In order to capture the content, a pirate needs only to record a picture directly from a high-definition TV.

**Figure 4: Number of UGC live streaming sites showing English Premier League Games**



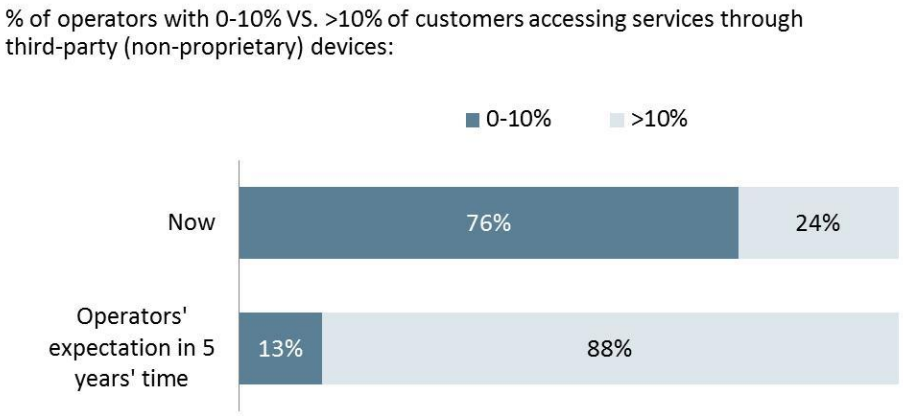

*Source: NetResult, Update on Digital Piracy of Sporting Events 2011*

[3] Farncombe's Security and Piracy Survey was conducted during August and September 2012 across a panel of over 200 industry experts including broadcasters, content owners, pay-TV operators, middleware/security vendors and device manufacturers. See: http://bit.ly/Ne1pPk

### Multiscreen distribution

Farncombe's Security and Piracy Survey also demonstrates how operators are increasingly enabling the distribution of content to third-party devices which are not in their control. As this becomes more common, responsibility for security moves outside the scope of the broadcast network – each additional non-proprietary device supported creates another point of attack for pirates from which to source high-quality content. As most of these devices are connected, their security is not discussed in this paper.

**Figure 5: Use of third-party devices by pay-TV operators**




*Source: Farncombe Security and Piracy Survey*

## 2.2 Changing focus of security

The weak points of a pay-TV operation are changing. Hackers will try to pursue the highest return on investment, which will come from targeting content directly, be it from the TV screen itself or from the distribution of content among the increasing number of multiscreen devices.

The focus of security needs to change, therefore, from protecting the distribution of content, to monitoring, identifying and prosecuting pirates.

This creates the need for a new set of technologies that allow operators to locate and shut down the sources of piracy. Such technologies include:

- Content watermarking
- Content fingerprinting
- Internet monitoring

Descriptions of these technologies are given in Figure 6 overleaf.

**Figure 6: New anti-piracy technologies**

| | |
|---|---|
| **Watermarking** | Watermarking embeds indelible and imperceptible data within the audio or video. Watermarking may be applied at any stage in content distribution, from creation to device-based watermarking, allowing for greater levels of granularity in detecting the source of the content. |
| **Fingerprinting** | Fingerprinting, not to be confused with overt watermarking (such as the visible display of a device unique address or the name of the operator distributing the content, which is sometimes also referred to as fingerprinting), allows video to be identified by comparing the fingerprint generated from a video segment and stored in a database before distribution with the one calculated on receiving the video. This process allows for automated, rapid comparison of multiple video streams on a single server. |
| **Monitoring** | Monitoring helps identify and locate pirate activity and encompasses a range of activities: Behavioural analysis looks for anomalous behaviour and network activity; Protective monitoring looks for attack patterns in network, firewall, ADS and IDS data not visible at a lower level; Web monitoring searches for illegal activity across the web. |

*Source: Farncombe*

# 3. The Total Cost of Ownership of CA Systems

## 3.1 Analysis of card-based and cardless systems

### Overview

Farncombe's Total Cost of Ownership (TCO) model for CA systems is designed to help operators understand the cost drivers that impact their choice of CA system.

The costs of setting up a CA system, though varying widely among security vendors, are generally well-understood and can, at the least, be anticipated through a vendor selection process.

However, over the lifetime of a CA system, set-up costs are likely to represent under half the total cost of running the system. Maintenance, additional CRM logistics and updating or replacing devices in response to security breaches must also be taken into consideration when selecting a CA system.

### Cost components and Cost drivers

Farncombe has identified and modelled components of cost throughout the CA system lifecycle, for card-based and cardless systems, as summarised in Figure 7. The key variables that drive these costs are shown in Figure 8.

**Figure 7: Key cost components**

| | |
|---|---|
| **Set up costs** | Includes device integration, CRM integration, headend equipment, licences, device components and, in the case of card-based systems, the cost of smartcards and their distribution. |
| **Operational costs** | Includes CRM overhead, additional call-centre volume, cost of delivering CA data and other maintenance of the system. |
| **Hack response costs** | Includes cost of developing and distributing software updates and replacing devices where necessary. |

*Source: Farncombe*

**Figure 8: Key drivers**

| | |
|---|---|
| **CA system type** | Card-based vs. cardless |
| **Network type** | DTH, DTT, Cable |
| **Total device base** | Annual and cumulative number of customer devices (including effects of churn) |
| **Rate of attack** | e.g. high-value services will experience a more frequent rate of attack |
| **Device variants** | Number of device variants in customer base (including software variants) |
| **Perfect clone attack** | Does an operator suffer a perfect clone attack? |

*Source: Farncombe*

## Illustrative results

In Figure 9 we show three possible CA implementations for a DTH operator with one million subscribers. These implementations are:

1. A smartcard CA system
2. A cardless CA system with a smartcard slot (for use in the case of a perfect clone attack)
3. A cardless CA system without a smartcard slot

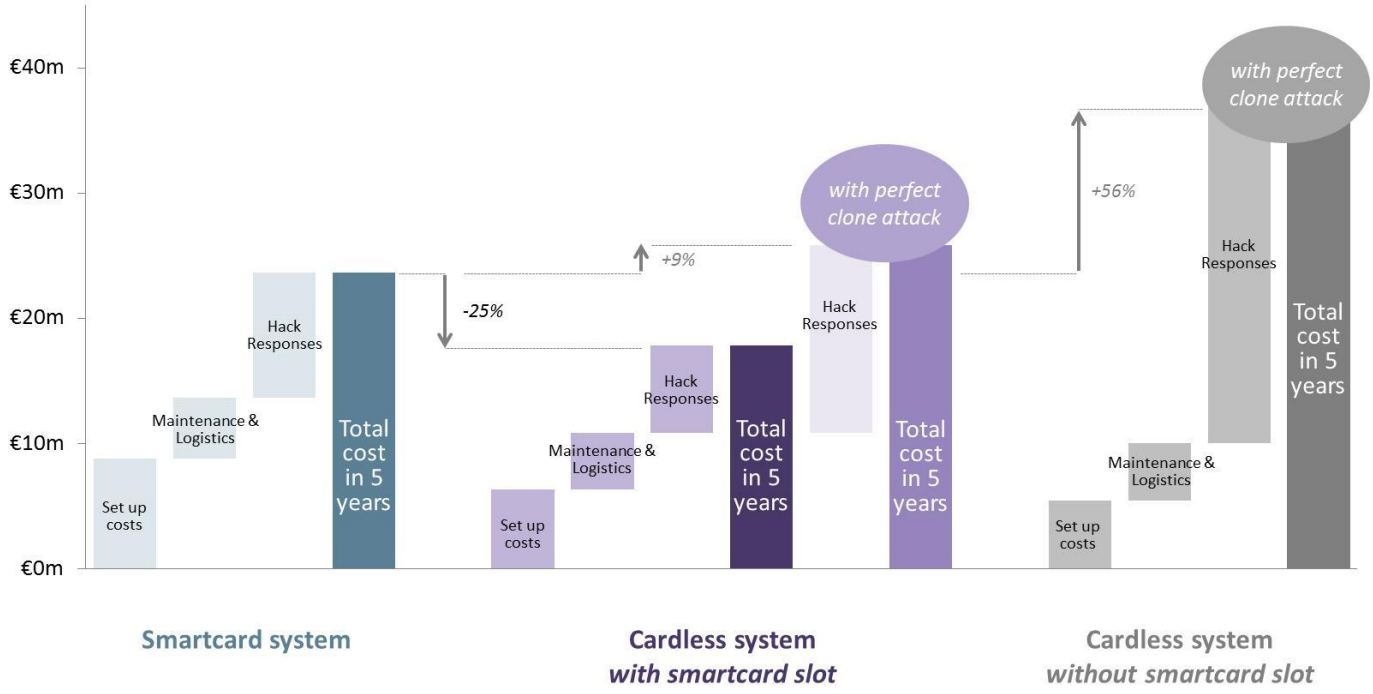
In this model the cost of the cardless CA system over 5 years is 25% less than that of the smartcard system. These savings arise out of reduced logistics costs and from eliminating the need for the smartcard itself.

For the cardless implementations, we have shown the effect of a perfect clone attack on the total cost of ownership: if a slot is present, the cost of distributing smartcards to the subscriber base is modelled; if a slot is not present, the cost of replacing all devices (at an average cost of €20 per subscriber) is modelled.

These results reinforce Farncombe's view that a smartcard slot should be provided as mitigation against the risk of a perfect clone attack.

Whilst for many operators the likelihood of a perfect clone attack may be low (as previously discussed in this paper) the cost of including a smartcard slot is minimal.

**Figure 9: Total cost of ownership of CA system for pay-DTH operator with 1m subscribers (€m)**




*Source: Farncombe*

## Impact of other variables

These examples show a specific operator case, though one that is representative of that experienced by many operators. Farncombe's model shows that platform type (specifically the cost of bandwidth), variants of device, churn-rate and likely frequency of attack all have significant implications for the total cost of ownership of both card-based and cardless systems.

Operators should understand these variables fully before making a decision on the implementation of a CA system.

# 4. Conclusion

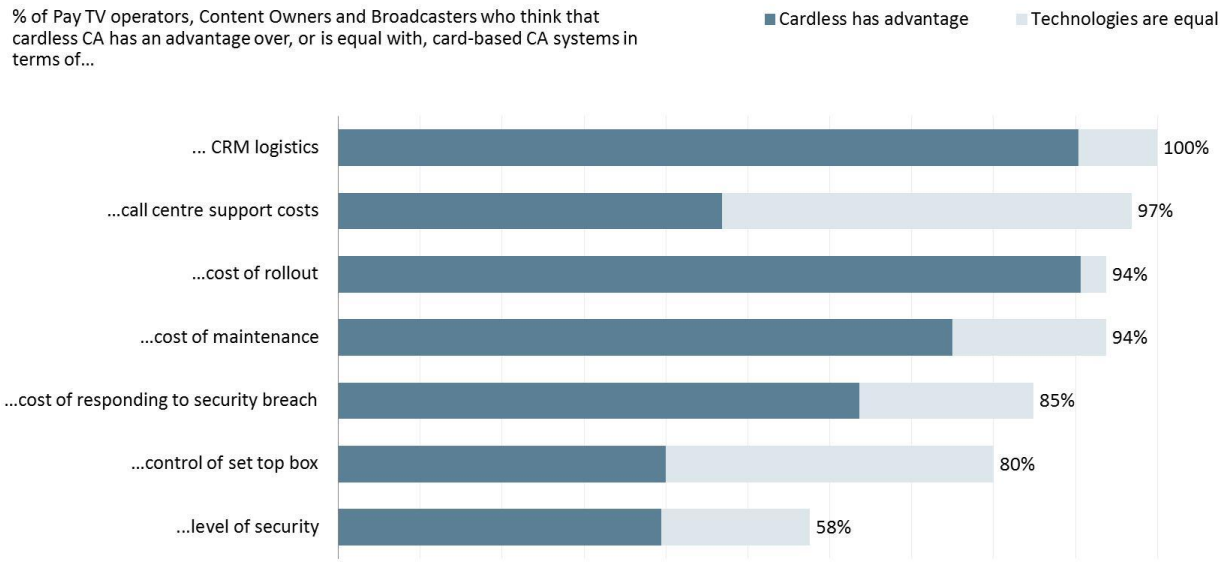
## 4.1 The status and future of cardless CA systems

Farncombe's Security and Piracy Survey shows a clear perception among operators and content-owners that cardless CA systems have several operational advantages, including logistics, call-centre support costs, rollout cost and maintenance costs (see Figure 10). A slight majority of the industry, however, still perceives cardless CA systems as less secure.

This paper argues that new security technologies lift the barriers to hacking cardless systems as high as those to hacking card-based systems, as long as they are implemented correctly.

However, no broadcast CA system can provide barriers high enough that they will not eventually be overcome – hacking equipment will advance while security is fundamentally limited by the hardware used in its original deployment. In a smartcard system, this is mitigated for by the ability to swap smartcards – in a cardless system, there is no such mitigation available.

**Figure 10: The advantages of cardless CA systems according to the TV industry**




*Source: Farncombe Security and Piracy Survey*

## 4.2 A changing security environment

Despite our assertion that serious pirates will always be able to keep up with improvements in security, we believe that the cost of doing so will remain high for well-designed systems. The investment in hacking required of a pirate must be justified by the return of the hack. Given the increasing ease of content redistribution and the creation of new weak points in a multiscreen environment, we expect the focus of piracy to shift away from the hacking of broadcast networks, except in the case of operators that continue to provide a high-value opportunity to the pirate (i.e. those with premium content and a large reach).

Operators with a low volume of premium content or a low reach should expect the frequency with which their CA system is attacked to decrease as piracy focus turns to content re-distribution. Nevertheless, in time today's systems become tomorrow's legacy systems and will become easier for pirates to exploit as technology advances.

The desire of pirates to attempt a perfect clone attack on a cardless CA system (which would force STB replacement) will drop, as the benefits to pirates reduce. However, pirates will attack systems as a challenge, so

as new tools become available to the pirates there will be a balance between the ability to attack a system and the ease with which a system may be attacked. Farncombe's Security and Piracy Survey showed cloning as operators' lowest concern, which suggests that there is already a reduced interest in attacking systems directly.

## 4.3 Appropriate use of cardless CA in a one-way network

Farncombe therefore concludes that there may be scenarios in which the use of a cardless CA system is appropriate in a one-way network. These include:

1) Where the operator has a low reach (low potential customer base for the pirate);
2) Where the operator has a low volume of premium content that is not available elsewhere;
3) In markets with high broadband penetration and speeds;
4) For free-to-air services applying geographical restrictions.

These scenarios are where incentives for pirates to attack the network are low, as long as barriers to hacking are kept sufficiently high.

While we believe the use of cardless CA is appropriate in these scenarios, **we recommend the inclusion of a smartcard slot** as a precaution to mitigate the risk of having to replace all devices (given the low cost of the inclusion of a slot and the high cost of device replacement). However, the smartcard system cannot offer protection against a control-word sharing or content re-distribution attack in this case.

## 4.4 Actions for operators considering a cardless system

We have named several scenarios in which we believe the use of a cardless CA system may be appropriate in a one-way network. Operators however must always consider their unique conditions before purchasing a CA system. The checklist in Figure 11 is a starting point for operators considering using a cardless CA system in their one-way broadcast network.

In addition to setting up an effective CA system, operators must implement technologies that enable the direct fighting of content redistribution and control-word sharing, such as watermarking, fingerprinting and monitoring.

For more information on any how to implement any of the solutions described in this paper, please contact Farncombe.

**Figure 11: Cardless checklist**

| | |
|---|---|
| ➢ | **Evaluate your risk profile:** How likely are you to suffer from content redistribution, control-word sharing or cloning? |
| ➢ | **Manage your devices**: Do you have a tightly-managed device population? What are the device memory and CPU requirements for the cardless CA system now – and what are they anticipated to be in 5 years' time? |
| ➢ | **Understand your vendor's solution:** Is the vendor's selection of SOCs appropriate for your devices? Has the CA system vendor properly certified the SOC? Has the CA system vendor made use of generic security features or employed the latest technology? |
| ➢ | **Know your CA vendor roadmap:** Does the CA system vendor have a development programme that allows it to roll out a wholly new software design? Does it have the funding and resources to do that? |
| ➢ | **Think about multiscreen:** Is the cardless CA solution partially or wholly portable between different device-types? |
| ➢ | **Prepare for the cost of updates:** What bandwidth is required to support minor and major software updates, including obfuscation and secret data? How much does your bandwidth cost you? |
| ➢ | **Understand the threat to your CA system:** Can the CA system vendor assure you that the breach of one device will not result in the breach of many or all devices? Is content re-distribution or control-word sharing a significant threat? |
| ➢ | **Check your contract:** What warranty is offered? What level of security warranty is offered in terms of time to breach and compensation for a breach? |

*Source: Farncombe*

# 5. About Farncombe

Farncombe is a leading provider of specialist strategy, technology consultancy and engineering services to the digital TV industry, with a global reputation in the content security field. With offices in the UK, France and Germany, Farncombe's roster of clients includes many of the world's leading broadcasters, platform operators, telecom operators, hardware and software technology providers as well as government and regulatory bodies, private equity companies and other industry stakeholders.

Farncombe's Security Practice is an internationally recognised advisor to pay-TV and connected TV players, providing security audits, a security monitoring service and consulting. For further information visit **http://www.farncombe.com/practices/content-security/.** You can also register to receive news updates and White Papers at **http://www.farncombe.com/news/.**

Liberty House
222 Regent Street
London W1B

**T** +44 (0)207 297 2002
**F** +44 (0)207 207 2100
**e:** security@farncombe.com
**www.farncombe.com**

# About Verimatrix

Verimatrix specializes in securing and enhancing revenue for multi-screen digital TV services around the globe. The award-winning and independently audited Verimatrix Video Content Authority System (VCAS™) and ViewRight® solutions offer an innovative approach for cable, satellite, terrestrial and IPTV operators to cost-effectively extend their networks and enable new business models. As the recognized leader in software-based security solutions for premier service providers, Verimatrix has pioneered the 3-Dimensional Security approach that offers flexible layers of protection techniques to address evolving business needs and revenue threats. Maintaining close relationships with major studios, broadcasters, industry organizations, and its unmatched partner ecosystem enables Verimatrix to provide a unique perspective on digital TV business issues beyond content security as operators seek to deliver compelling new services. Verimatrix is an ISO 9001:2008 certified company. For more information, please visit www.verimatrix.com, our *Pay TV Views blog* and follow us at *@verimatrixinc*, *Facebook* and *LinkedIn* to join the conversation.

To download the paper from the Verimatrix website, visit **www.verimatrix.com/cardless**

# 6. Appendix – Cardless and Card-based Technology

## 6.1 Cardless and Card-based protection against hacking

### Smartcard-based CA systems: overview

Since the late 1980s, the most prevalent form of CA system in one-way broadcast networks has been that using smartcards. The smartcard contains a system-on-chip (see below), which contains the core of the proprietary security implementation. The main reason for using a smartcard solution is that, if the smartcard is hacked, it can be replaced without having to replace the entire reception device (unless the attack is such that it forces a device replacement even for a card-based system).

### Cardless CA systems: overview

Cardless CA systems, previously only used in two-way networks (those which have an always-on return path, such as IPTV or internet-enabled cable networks), are now also being used in one-way networks. In two-way networks, these software-based solutions perform validation of the customer's right to view content in the security headend – a secure one-to-one channel can then be set up between operator and customer through which to deliver the content.

These software-only based systems, however, are not suitable "as-is" for use within a one-way network, as no secure channel can be set up – the same content with the same encryption and the same encryption key must be broadcast to all customers, and validation of the customer's right to view must be done in the device.

***System on Chip (SoC):*** An SoC can be thought of as a mini-computer contained on a chip. In the security systems discussed in this paper, the SoC is responsible for performing key management operations and, when deployed in the form of a uniquely personalized device, provides an implementation-specific root of trust, and one or more securely-held secret keys unique to each device.

In theory it would be possible to employ a cardless system which implements the whole security solution within the immutable part of the SoC. This would effectively be the same as embedding a smartcard in the device and assuming it would never have to be replaced. As we expect smartcards to need replacing over time, this is a flawed solution.

**In Farncombe's view, the only type of cardless CA system viable for use in a one-way network is one in which the system is implemented with part of the functionality in the main processor and part in the SoC.** In this combined architecture, the unique elements of the system, such as the root of trust, should be provided by the secure processor within the SoC – and the generic elements, such as processing of any common data such as content keys, in the main processor.

*In this paper, where we discuss cardless CA systems, we are referring to those with **a combined software and hardware implementation** as described above.*

### Key differences in protection against threats

The key differences between the protection provided by card-based and cardless solutions are as follows:

1) **Protection against control-word sharing**. Wherever the common key (control-word) used to decrypt content is used in a CA system, it must be well protected. If the control-word can be found or generated, a control-word sharing attack is possible. This applies equally whether the control-word is being used in the software and hardware of a cardless system, or the hardware of a card-based system. However, in a card-based system there has to be an external interface between the smartcard and the device, over which the control-word must be passed, providing a weak point for the pirate to attack. In cardless systems, the only interfaces are internal – if implemented correctly, an internal interface should be easier to protect than an external interface.

2) **Protection against cloning**. Both card-based and cardless systems can suffer a *partial* clone attack, where part of the security functionality is discovered and distributed such that users of the cloned parts are able to extract control-words from the broadcast signal on a standalone basis, without a permanent internet connection. However, in a card-based system, the attack can always be stopped through a software update or smartcard replacement (depending on the exact nature of the attack). In a cardless solution, though, it is possible to produce a *perfect* clone which can follow all software updates. If the operator can discover the identity of the cloned device, it can switch that device off, but if a new identity can be easily discovered (cloned), the pirate can distribute the new identity and the hack will continue to work. In this situation, the only remedy is to replace all devices in the subscriber base.

It should be noted that neither system provides protection against the first threat we described in Figure 2, that of **content redistribution**.

## How are CA vendors improving protection?

The challenge for vendors of both card-based and cardless CA systems is to sustain the level of resistance to attacks that they provide. There are a number of new techniques that allow them to do this, the most important of which are described in Figure 12. Each of these technologies is evolving and improving. However, as described in the next section, pirates' technology will improve in parallel. Use of these technologies is therefore a requirement for future CA systems, but will not prevent pirate attacks outright. It is likely that the use of these technologies will continue to improve the quality of cardless systems.

**Figure 12: New technologies in CA**

| | |
|---|---|
| **White box cryptography** | White Box Cryptography (WBC) is a technique that transforms cryptographic algorithms from a traditional implementation into a series of tables and lookups, making reverse engineering and key discovery far more difficult. WBC can be done for most of the popular symmetric and asymmetric cryptographic algorithms. |
| **Software obfuscation** | Software obfuscation is a series of techniques that transforms control and data structure code into a structure that is hard to reverse-engineer (or decompile to something readable) by machine or human means. Simple steps are to remove sensible naming and descriptors from the code (which give a hacker 'hints' as to what is happening), through to more complex methods which split, flatten and merge arrays, substitute code for static data, etc. Software obfuscation alone only makes an attacker's task more difficult, and should never be relied on as a measure on its own. |
| **Chip set Camouflaging (hiding gates)** | Silicon vendors tend to use standard cell libraries when fabricating their chips, in particular silicon geometry. However, with university-level equipment such as electron microscope interrogation, gate-level structures can be viewed and – eventually – the logical function reverse-engineered. There are steps that can be taken to introduce gates that look the same as other gates that do the same logical function, dummy gates, and so forth. This makes a hardware-level reverse-engineering process more difficult. |
| **Glitch, power and DPA analysis, and EMC resistance** | The smartcard industry has for years had to be resilient against attacks which attempt to infer information about the device by monitoring electromagnetic radiation (EM) given off, fluctuations on the power-supply rails (simple and differential power analysis) and glitch analysis (disturbing the circuit with focused ions or electrical impulses so as to make the hardware 'jump' to a non-intended state of operation). Mitigation against these types of attack is starting to be required in the wider electronics industry, for instance by using 'non-standard' implementations of cryptographic algorithms which do not use secret values 'wholesale' in their mathematics, or by designing hardware state machines to be more resistant against glitch disturbances. |
| **Software Isolation** | Because software provides ultimate flexibility in the field it is preferred. However modern devices have open application environments where sensitive code modules must be isolated (or 'sandboxed') such that either malware or unintended bugs in the open environment cannot be used to uncover methods, content or secret keys from the secure code. Silicon and IP vendors now provide mechanisms to hive off secure code-segments into logically distinct areas, such that only they can access certain areas of memory or key stores. |

*Source: Farncombe*

## 6.2 Hacking a CA system: A pirate's point of view

### Barriers to hacking

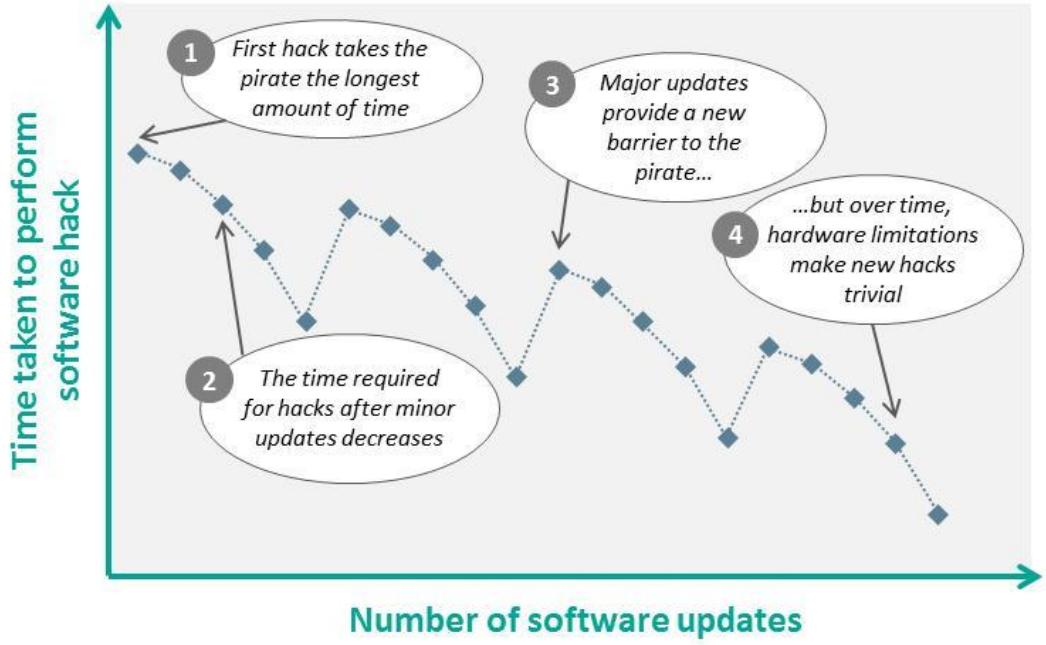
The nature of technology improvement means that it is impossible to create a security system for a one-way broadcast network that a pirate is never able to hack. The fact that security functionality must reside in the end-user's device means that it can only make use of the hardware present in the device at the time of manufacture.

As the technology available for attacking this hardware continues to develop, the task of hacking the device becomes trivial (to a pirate with access to the latest technology).

In general, then, a CA system in a broadcast network which is under constant attack will have a finite lifetime. During this time the operator can perform software updates which cause the pirate to have to re-hack the system. These updates will vary in the number of new tools they use: the more major an update is in terms of new functionality, the greater a barrier it will pose to the pirate re-hacking the system. Eventually though, the hardware in the device will limit the new functionality possible and the barrier to hacking will be removed.

This declining barrier to hacking is illustrated in Figure 13. This profile of declining hacking time applies to the hacking of software and software updates – generally, when the hardware itself is hacked for the first time, updates will do little to prevent subsequent hardware hacks.

**Figure 13: Decreasing barriers to hacking software systems over time**




*Source: Farncombe*

### Resources required: when is a hack worth doing?

Different types of hack require different resources:

1) **Software hack** – requires processing-power and time
2) **Hardware hack** – requires access to advanced (and costly) technical analysis equipment
3) **Complete system hack** – requires access to all of the above

Performing a hack must be worthwhile to the pirate. Advanced CA systems may require investment in the order of hundreds of thousands of dollars to hack, with further investment required for each subsequent hack.

A pirate is only likely to invest in such hacks on high-value broadcast networks (i.e. those with premium content and a large reach) so that the investment can be recovered through sales of clones or subscription to a control-word sharing service. Conversely, a lower-value network, with low reach or little premium content, will only be

worth hacking once the cost of hacking the network is low enough. These lower-value networks are likely, therefore, to experience a lower rate of hacking than higher-value networks.

### Maintaining a pirate service

As with the cost of performing a hack, the cost of running a pirate service depends on its nature. Looking at our three categories of piracy threat, the drivers of costs are as follows:

1) **Content redistribution** – cost driven by the distribution of content over the internet. This may mean streaming from dedicated server, distributing through a CDN, using a free live streaming service or using P2P distribution.
2) **Control-word sharing** – cost driven by maintenance of internet connection and control-word server.
3) **Cloning** – one-off cost to distribute clones and occasional cost of distributing updates.

The pirate must also have a guaranteed income from his activity. This prospect may decrease over time with the increased amount of content available for free on illegal web sites, cyber-lockers or P2P networks – even before such content appears on pay-TV channels.

## 6.3 Responding to hacks: An operator's point of view

### The need for a response

There are two main reasons for operators needing to respond to hacks:

1) Impact on revenues
2) Pressure from owners of premium content

Exactly how a hack impacts on operator revenues can vary greatly, but it is important to note that a pirate's business shares many similarities with the operator's. The pirate offers a service which must consist of an attractive product proposition at a price that represents good value for money. This service needs advertising to encourage take-up, which will happen over time. The speed of take-up of the pirated service will also depend on factors such as fear of prosecution and culture of the region – indeed, early adopters of the pirated service are likely to be those consumers who are unwilling to pay for a service at all.

It may therefore take some time after a service is hacked before the operator sees any real impact on revenues, which happens when paying customers begin to churn from the platform in order to take the pirated service. Additionally, many customers are committed to contracts of 1 year or more, limiting the speed at which they can cease payments.

For most operators, it is likely that the primary source of pressure to respond to a hack will come from premium content providers, which usually have strict clauses in rights contracts with respect to security.

### Types of response

We have considered three types of responses to attacks, ordered in increasing cost to the operator.

#### *Shut-down of pirate service*

For many operators who suffer a security breach, taking steps to shut down the pirated service will be a sufficient response. It will deny the pirate the ability to offer a consistent service and discourage take-up – it may also lead to successful prosecutions of pirates themselves.

However, the ability to shut down a pirate service is restricted to the threats of content redistribution and control-word sharing. Cloning cannot be effectively shut down as, once the clone has been sold (for an upfront payment), no maintenance is required by the seller. Clones that reveal their identity can be detected and disabled, however if new clones can be developed rapidly or their identity is hard to find then the threat cannot be removed.

The prevalence of content redistribution and control-word sharing as threats makes the "shut-down" approach increasingly relevant. This is leading to the development of a range of technologies designed to enable this approach, such as watermarking, fingerprinting and monitoring. These are discussed in Section 2.2 of this paper.

***Security updates***

Once piracy has reached a sufficient scale, or when requested by a content provider, security updates are necessary. These involve developing and distributing new software which must be successfully installed on all devices.

***Device replacement***

In the case where a hack cannot be stopped through a security update, the operator must replace devices. For a card-based CA system this usually means performing a smartcard swap (replacing all smartcards in the customer base), or in the case of a control-word sharing attack, replacing devices (though most operators would attempt to shut down the pirate service before resorting to this). For a cardless CA system, this always means replacing all customer devices.